UNITED STATES DISTRICT COURT

for the

Northern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
A Black LG Smartphone Bearing Serial Number ZNFL555DL, Containing a SanDisk 64 GB Micro-SD Card; a Green and Gray 32 GB Micro-SD Card; a 2 GB PNY Blue SD Card; and a Sony Vaio Laptop Bearing Serial Number 27524532 3017993; All Located in FBI Binghamton Resident Agency, 15 Henry Street, #321, Binghamton NY 13901

Case No. 5:21-MJ - 220 (ML)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
A Black LG Smartphone Bearing Serial Number ZNFL555DL, Containing a SanDisk 64 GB Micro-SD Card; a Green and Gray 32 GB Micro-SD Card; a 2 GB PNY Blue SD Card; and a Sony Vaio Laptop Bearing Serial Number 27524532 3017993; All Located in FBI Binghamton Resident Agency, 15 Henry Street, #321, Binghamton NY 13901
located in the Northern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2)(A) & (a)(5)(B)	Receipt and Possession of Child Pornography

The application is based on these facts:
See attached affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

ATTESTED TO BY THE APPLICANT IN ACCORDANCE WITH THE REQUIREMENTS OF RULE 4.1 OF THE FEDERAL RULES OF CRIMINAL PROCEDURE.

Applicant's signature

Jenelle Corrine Bringuel, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 04/16/2021

Judge's signature

City and state: Binghamton, New York

Hon. Miroslav Lovric, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jenelle Corrine Bringuel, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent of the United States Department of Justice, Federal Bureau of Investigation ("FBI"), and I am empowered by law to investigate and make arrests for offenses enumerated in 18 U.S.C. § 2516. As such, I am an "investigative or law enforcement officer" within the meaning of 18 U.S.C. § 2510(7).

2. I have been employed as a Special Agent of the FBI since June 2012 and am currently assigned to the Albany Division, Binghamton Resident Agency. While employed by the FBI, I have investigated federal criminal violations related to cybercrime, child exploitation, and child pornography. I have gained experience through training by the FBI and the investigations in which I have personally participated. I have participated in the execution of several federal search warrants in child sexual exploitation investigations.

3. I am currently investigating Matthew Bormann who I suspect has knowingly received and possessed child pornography, in violation of 18 U.S.C. § 2252A(a)(2)(A) & (a)(5)(B) ("Subject Offenses").

4. This affidavit is submitted in support of a warrant to search (1) a black LG smartphone bearing serial number ZNFL555DL, containing a SanDisk 64 GB micro-SD card, (2) a green and gray 32 GB micro-SD card, (3) a 2 GB PNY blue SD card, and (4) a Sony Vaio laptop bearing serial number 27524532 3017993 (collectively, "Subject Electronic Devices") that the United States Probation Office for the Northern District of New York ("Probation Office") seized from Bormann's residence on March 12, 2021. The Subject Electronic Devices are currently located at the FBI Binghamton Resident Agency, 15 Henry Street #321,

Binghamton, NY.

5. The statements and facts set forth in this affidavit are based in significant part on my review of written documents obtained from the United States Probation Office, conversations with probation officers, and my personal training and experience. Since this affidavit is being submitted for the limited purposes of a securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts and circumstances that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the Subject Offenses are presently located on the Subject Electronic Devices.

BACKGROUND OF THE INVESTIGATION

6. On August 18, 2015, Bormann was sentenced in the United States District Court for the District of South Carolina to 36 months' imprisonment and a life term of supervised release related to his prior guilty plea to one count of possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) & (b)(2).

7. On May 1, 2018, Bormann began his term of supervised release. On August 14, 2018, the Northern District of New York accepted a transfer of jurisdiction for Bormann's supervised released. On March 6, 2020, Bormann reported to the United States Probation Office (Probation) office for a scheduled office visit and was questioned about his access to computer and internet devices. Bormann admitted that over the summer months of 2019, he accessed a computer at the Sherburne Public Library for the purposes of seeking employment. He also stated that he last used a computer at the library sometime in the beginning of February 2020. Bormann admitted he had not received authorization from his probation officer to access the Internet on a computer at this location. Bormann was admonished by Probation, and his

probation officer (PO) reviewed with Bormann his conditions of supervised release and the restrictions related to accessing the Internet or a computer device. Bormann attested he was only using the Internet for job searching and no other purpose. Bormann's PO subsequently reviewed the Sherburne Library public web page which advertises that the library contains a children's room that supports recreation, pre-teen book club, story time, and a summer reading program for children. In direct response to his unauthorized use of the Internet and concerns of Bormann having unsupervised contact with minors at this location, Bormann was instructed by his PO to no longer frequent the Sherburne Public Library.

8. On March 6, 2020, Bormann's supervised release conditions were modified by Senior United States District Judge Thomas J. McAvoy. These modifications included the special condition that Bormann "must not use or possess any computer, data storage device, or any internet capable device unless [he] participate[s] in the Computer and Internet Monitoring Program (CIMP), or unless authorized by the Court or the U.S. Probation Office." The same special condition further states that Bormann "must permit the U.S. Probation Office to conduct periodic, unannounced examinations of any computer equipment, including any data storage device, and internet capable device [he] use or possesses" and that "[t]his equipment may be removed by the U.S. Probation Office or their designee for a more thorough examination." A separate special condition of Bormann's supervised release states that Bormann:

> must submit [his] person, and any property, house, residence, vehicle, papers, effects, computer, electronic communications devices, and any data storage devices or media, to search at any time, with or without a warrant, by any federal probation officer, or any other law enforcement officer from whom the Probation Office has requested assistance. Any items seized may be removed to the Probation Office or to the office of their designee for a more thorough examination.

9. On the same day, March 6, 2020, Bormann was presented with the above-described modifications to his supervised release conditions, which were also explained to him by counsel, and Bormann signed off on the modifications.

10. On March 12, 2021, Senior United States Probation Officer (Sr. USPO) Michael Christopher and PO Nicole Cotugno conducted a home visit at Bormann's residence. The POs were greeted at the door by Bormann's mother who stated Bormann was sleeping. PO Cotugno asked her to wake him. Bormann's mother went upstairs and then called the POs up when Bormann was awake. Bormann's mother subsequently left the room where Bormann had been sleeping. While PO Cotugno was talking to Bormann, Sr. USPO Christopher looked around the room for anything in plain sight. Bormann was asked about a PS4 game system and if he connects to the internet and he denied doing so. While PO Cotugno was speaking with Borman, both POs noticed a black smart phone on the couch where Bormann had been sitting. The smart phone was later identified as an LG L555DL. Bormann was questioned about the smartphone and stated it was mother's phone. Bormann then grabbed the phone and tried to leave the room with it and stated he was returning it to his mother. PO Cotugno stopped him and said that the PO would give it back to her and took the phone. PO Cotugno asked Bormann if it was his phone and he continued to deny ownership and stated he didn't know the passcode needed to unlock the phone. PO Cotugno reminded him that per his conditions he was required to answer truthfully. Bormann continued to deny the phone was his. Sr. USPO Christopher then noticed the charging cord next to the couch where Bormann had been sleeping and PO Cotugno plugged the cell phone in to show that it was the cord for the phone. Bormann continued to deny the phone was his and insisted it was his mother's phone. PO Cotugno left Sr. USPO Christopher in the bedroom with Bormann and found Bormann's mother downstairs in the living room. PO

Cotugno asked Bormann's mother where her phone was. In response, Bormann's mother showed PO Cotugno that her phone was on the stand in the living room. PO Cotugno asked Bormann's mother if she recognized the cell phone that PO Cotugno had taken from Bormann's room and she said "no." Bormann's mother returned to the bedroom with PO Cotugno and asked Bormann about the phone. Bormann stared at his mother and told her that the phone found in the room where he was sleeping was hers, but Bormann's mother would not agree. Bormann finally admitted that the phone was his and that he had possessed it for a "few months." Bormann gave PO Cotugno the passcode to unlock the phone. PO Cotugno asked Bormann if she would find anything related to him on the phone or anything inappropriate and he said no. Later he admitted that PO Cotugno would find "appropriate"-aged pornography on the phone.

11. Sr. USPO Christopher asked Bormann if he consented to Probation searching his room and Bormann consented. Bormann was asked to sit in a chair while the room was searched. Sr. USPO Christopher reviewed the PS4 device and found the PS4 had been used to search the Internet for pornography, and that Bormann had visited pornhub.com where he had viewed pornography.

12. During the search, PO Cotugno also found two SD cards in the nightstand next to Bormann's bed—a green and gray 32 GB micro-SD card and a blue 2 GB PNY SD card—along with a small notebook that had websites written in it. PO Cotugno checked under Bormann's bed and found a Sony Vaio laptop computer bearing serial number 27524532 3017993. This was the same laptop that had previously been returned by Probation to Bormann without CIMP software installed after finding that the device was too old to run the CIMP software described in Bormann's modified release conditions. When the laptop was returned to Bormann by Probation, however, Bormann was told that he could not use it without the CIMP software installed.

Initially Bormann denied using the computer and denied connecting it to the internet. He later admitted to using it approximately three weeks prior. Because the USPO had not given Bormann permission to possess any of the devices and none were enrolled in CIMP. PO Cotugno seized the cell phone (LG L555DL), PS4, the laptop, notebook, the two SD cards, and a Wii game console that was also found. PO Cotugno transported the items to Probation's Syracuse Office.

13. On March 15, 2021, Senior United States Probation Officer (Sr. USPO) Scott Shanahan conducted a Cellebrite exam of Bormann's LG L555DL smartphone that was seized by PO Cotugno as an unreported and unapproved internet capable device, in violation of his computer monitoring conditions. Although it became apparent during the extraction of the LG L555DL, based on the age of the device and the fact that the model of device was not natively supported by Cellebrite[1], that not all relevant data was extracted from the device, the extraction process did identify a large quantity of child exploitation material on the device. Sr. USPO Shanahan reviewed the material and found that it included still images and videos of children under the age of 18 involved in lewd and lascivious displays of their genitalia as well as the oral, anal, and vaginal penetration of minor children by adult or minor male penises, sex toys, or other objects. The fact that the LG L555DL was not natively supported during this initial Cellebrite extraction is the primary reason that your affiant seeks the requested warrant; so that another extraction may be performed to ensure all relevant data is recovered from the device.

14. Sr. USPO Shanahan provided your affiant with the following information about his review of the information he was able to extract from the phone: The images and videos depict both pre- and post-pubescent children. One image, "1600369317509.jpg," depicts what

[1] Cellebrite is a software package used by law enforcement for the purpose of extracting the contents to cellular telephones.

appear to be a minor female and a minor male wherein the minor female is performing oral sex on the minor male. One video, entitled "Hermanas Putibuenas (64).mp4" depicts what appears to be a minor female masturbating with a carrot. This video appears to be part of a series of videos also found on the device with similar titles that all appear to be of the same or a similar minor female engaging in masturbatory acts. A manual review of Cellebrite extraction also revealed two email addresses associated with Bormann were accessed with this phone.

15. Sr. USPO Shanahan also conducted a manual review, through a write blocking device[2], of the blue 2 GB PNY SD card and the green and gray micro SD card. The initial review of the green and gray micro SD card did not reveal anything noteworthy, but the review of the blue 2 GB PNY SD card revealed several images of computer screens showing websites with images of females who appeared to be under the age of 18 engaging in lewd displays of their genitalia. These images appear to have been taken by a camera. Despite the results of these initial searches, your affiant is seeking authorization to search both cards again in order to ensure all relevant evidence is recovered.

16. Sr. USPO Shanahan did not conduct a search of the Sony Vaio laptop bearing serial number 27524532 3017993.

17. On March 16, 2021, after noting the original phone extraction did not appear to recover all relevant data from the device, Sr. USPO removed the Sandisk 64-GB micro SD card from the LG L555DL smart phone and conducted a separate Cellebrite extraction of the SD card. The extraction from the SD card revealed a larger quantity of images and videos than had

---

[2] When reviewing the SD card and the micro SD card, the officers used a forensic computer program (also known as "write block") designed to ensure that they would not alter or delete any of the metadata associated with any of the files on the SD card.

previously been extracted when the SD card was inserted into the LG L555DL. An additional image extracted from the SD card, "1e4luuhq2x2.jpg," depicts three naked minor females where two of the girls are spreading the legs of the third girl to lewdly display her vagina. Video file "(Pthc) Nablot Smolianochki Stk2 10-13Yo (Bath,Dildo)-1.mp4" [3] appears to depict two minor females of approximately 10 and 13 years of age engaging in vaginal sex using a dildo.

COMPUTERS AND CHILD PORNOGRAPHY

18. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experiences and training of other law enforcement officers with whom I have had discussions, I know that computers, including desktop computers, laptops, SD cards, cellular telephones, and other electronic media, basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

19. A computer's ability to store images in digital form makes such devices an ideal repository for child pornography. The size of the electronic storage media used in computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. SD cards can also be used to copy, store, transport and transmit digital images.

20. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

21. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Gmail, among others. The

[3] I know, based on my training an experience, that distributors of child pornography frequently use the acronym "pthc," which stands for "pre-teen hard core."

online services allow a user to set up an account with a remote computing device that provides e-mail services as well as electronic storage of computer files with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

22. As with most digital technology, communications made from a computer are often saved or stored on that device. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer' web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a computer can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools.

23. I know that data files, including digitized images, correspondence, records, communications, and other matters sought by this Warrant, can be stored in a variety of digital formats on a computer using various software applications. For example, digital still images are commonly created and stored as JPEG files and identified by .jpg or .jpeg in filename suffix.

Digital still images may also be created, converted, or stored, among other things as an Adobe Acrobat file (using the suffix .pdf); embedded within a word processing document (using the suffix.wpd or .doc); or converted to another graphics file format (.gif or .tif). In addition, data filenames typically include a suffix associated with the application that created or modified the file (e.g., XXX.pdf indicates a file associated with Adobe Acrobat). A file name, however, can be manipulated to include a suffix that conceals its true format, or is not readily recognized by or associated with any software application. Accordingly, because digitized versions of items sought by this Warrant can be created and/or stored in any number of digital file formats, it is necessary to search every data file stored on a computer or other data storage device to locate and seize such items.

24. Mobile communication devices are commonly used for both personal and business use. These devices range from simple mobile telephones to complex devices encompassing numerous technologies in one hand-held device. They are electronically powered and typically combine the ability to store and transfer data along with serving as a communications facility. Mobile communication devices are essentially ultra-small computers, and in my experience, they are often a medium on which child pornography is stored. Mobile communication devices often include an SD card and users can sometimes select to have data on their mobile communication devices saved directly to an SD card.

25. Based on my training and experience, I know that mobile communication devices can be used to transmit both written messages (e.g., text messages) as well as images. Cellular telephones, for example, have the capacity to store voice mail messages, names, telephone numbers, addresses, sent and received text messages, and images in their internal memory. Many cellular telephones have the capability to capture digital photographic images and videos,

store them in internal memory or on SD cards, and transmit them to one or more different cellular telephones. I also know that individuals sometimes use cellular telephones to produce, send, and receive child pornographic images.

26. Based on my past experience and training, I know that persons who use computers in their homes tend to retain their personal files and data for extended periods of time even if a person has replaced, traded in, or "upgraded" to a new device. I also know personal computer users routinely transfer most of their saved data onto their new computers when making an upgrade. The data transfer is often done by saving files from the old computer to media sources (DVD's, USB flash drives, external hard drives, etc.), then opening them onto the new computer and saving them to the new hard drive. Visual images, such as child pornography, are as likely (if not more so) as other data to be transferred to a person's new, replacement, or upgraded computer system.

COLLECTORS OF CHILD PORNOGRAPHY

27. Individuals who are interested in child pornography may want to keep the child pornography files they create or receive for additional viewing in the future. Individuals who collect child pornography may go to great lengths to conceal and protect from discovery their collections of illicit materials. They often maintain their collections in the privacy of their homes, on computers, on external hard drives, on cellular telephones, or in other secure locations. Because the collection reveals the otherwise private sexual desires and intent of the collector and represents his most cherished fantasies, the collector rarely, if ever, disposes of his collection. The collection may be culled and refined, but, over time, the size of the collection tends to increase. Individuals who utilize a collection in the seduction of children or to document that seduction treat the materials as prized possessions and are especially unlikely to

part with them over time.

28. Individuals who collect child pornography may search for and seek out other like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also may help these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to: text messages, video messages, electronic mail, email, bulletin boards, IRC, chat rooms, newsgroups, instant messaging, and other vehicles.

29. Individuals who collect child pornography may maintain stories, books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children, as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals may keep these materials because of the psychological support they provide.

30. Individuals who collect child pornography may keep names, electronic mail addresses, cellular and telephone numbers, or lists of persons who have shared, advertised, or otherwise made known their interest in child pornography or sexual activity with minor children. These contacts may be maintained as a means of personal referral, exchange, and/or commercial profit. This information may be maintained in the original medium from which it was derived.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

31. I am trained in computer and cellular telephone evidence recovery and have extensive knowledge about the operation of cellular telephones and computer systems, including the correct procedures for the seizure and analysis of these systems.

32. Based on my knowledge, training, and experience, I am aware that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, transferred, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost to the user. Even when files have been deleted, they can be recovered months or years later using specialized forensic tools. This is so because when a person "deletes" a file on a computer or cellular telephone, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

33. Therefore, deleted files or remnants of deleted files may reside in free space or slack space—that is, in space located on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data or process in a "swap" or "recovery" file. Similarly, files viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache" located on the computer. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

34. Apart from user-generated files, an electronic device may contain electronic evidence of when it was used, what it was used for, and more importantly, who used it recently and in the past. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence or physical location. For example, registry information, configuration files, user profiles, e-mail address books, "chats," instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates and times) may in and of themselves be evidence of

who used or controlled the computer or storage medium at a relevant time in question.

SEARCH METHODOLOGY TO BE EMPLOYED

35. Searches and seizures of evidence from a computer commonly requires agents to download or copy information from those devices and their components or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computers can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computers for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and application, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an

operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

36. The search procedure for the Subject Electronic Devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data on the Subject Electronic Devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents and scanning storage areas;

e. performing key word searches to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

f. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

CONCLUSION

37. Based upon the above information, there is probable cause to believe that evidence of violations of 18 U.S.C. § 2252A(a)(2)(A) and (a)(5)(B), as outlined in Attachment B of this Affidavit, will be found within the Subject Electronic Devices. Therefore, based upon the information contained in this affidavit, I request that this Court issue the attached search warrant authorizing the search of the contents of the Subject Electronic Devices, set forth in Attachment A, for the items more particularly described in Attachment B.

ATTESTED TO BY THE APPLICANT IN ACCORDANCE WITH THE REQUIREMENTS OF RULE 4.1 OF THE FEDERAL RULES OF CRIMINAL PROCEDURE

Jenelle Corrine Bringuel
Special Agent
Federal Bureau of Investigation

I, the Honorable Miroslav Lovric, United States Magistrate Judge, hereby acknowledge that this affidavit was attested by the affiant by telephone on April 16, 2021, in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.

Miroslav Lovric

HONORABLE MIROSLAV LOVRIC
UNITED STATES MAGISTRATE JUDGE
NORTHERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to Be Searched

The property to be searched consists of:

(1) a black LG smartphone bearing serial number ZNFL555DL, containing a SanDisk 64 GB micro-SD card;

(2) a green and gray 32 GB micro-SD card;

(3) a 2 GB PNY blue SD card; and

(4) a Sony Vaio laptop bearing serial number 27524532 3017993

("Subject Electronic Devices").

The Subject Electronic Devices are in the custody of the FBI Binghamton Resident Agency, 15 Henry Street, #321, Binghamton NY 13901.

ATTACHMENT B

Items to Be Seized

Items and information that constitute fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2)(A) & (a)(5)(B) (Receipt and Possession of Child Pornography):

a. Any and all visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

b. Internet history, including evidence of visits to websites that offer visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

c. Chats, chat logs, emails, and other text documents, describing or relating to sexually explicit conduct with children, as well as fantasy writings regarding, describing, or showing a sexual interest in children.

d. Correspondence or other documentation identifying persons transmitting through interstate or foreign commerce, including by mail or computer, any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

e. Computer records and evidence identifying who the particular user was who received, downloaded, possessed, or accessed with intent to view any child pornography found on any computer or computer media (evidence of attribution), or who attempted to do any of the foregoing, and how the computer was used to effectuate that activity.

f. Correspondence and other matter pertaining to the receipt and possession of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256, and evidence that would assist in identifying any victims of the above-referenced criminal offenses, including address books, names, and lists of names and addresses of

minors, or other information pertinent to identifying any minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

g. Child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, and notes evidencing an interest in unlawful sexual contact with children, and evidence assisting authorities in identifying any such children.

h. Records showing the use or ownership of Internet accounts, including evidence of Internet usernames, screen names, or other Internet user identification.

i. Computer-related documentation that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

j. Any passwords, codes, or digital keys that provide access to any computer hardware, computer software, computer-related documentation, or electronic data records.

k. Documents and records regarding the ownership and/or possession of electronic media being searched.

This authorization includes all electronic data that falls within the above categories, including deleted data, remnant data, and slack space.